(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 0 942 849 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
31.01.2007 Bulletin 2007/05

(21) Application number: **97952440.2**

(22) Date of filing: **10.12.1997**

(51) Int Cl.:
B60R 16/02 *(2006.01)* ***G06F 11/00*** *(2006.01)*

(86) International application number:
PCT/US1997/023030

(87) International publication number:
WO 1998/026958 (25.06.1998 Gazette 1998/25)

(54) FAULT-RESILIENT AUTOMOBILE CONTROL SYSTEM

FEHLERTOLERANTES KRAFTFAHRZEUGSTEUERUNGSSYSTEM

SYSTEME DE COMMANDE PARA-DEFAILLANCE POUR AUTOMOBILE

(84) Designated Contracting States:
DE FR GB

(30) Priority: **16.12.1996 US 771343**

(43) Date of publication of application:
22.09.1999 Bulletin 1999/38

(73) Proprietor: **MICROSOFT CORPORATION**
Redmond, Washington 98052-6399 (US)

(72) Inventors:
- **WONG, William**
  Redmond, WA 98053 (US)
- **LEE, Lawrence, W.**
  Bellevue, WA 98007 (US)

(74) Representative: **Wright, Howard Hugh Burnby et al**
Withers & Rogers LLP
Goldings House,
2 Hays Lane
London SE1 2HW (GB)

(56) References cited:

EP-A- 0 033 664
EP-A- 0 277 302
EP-A- 0 434 907
EP-A- 0 793 084
EP-A- 0 793 156
EP-A- 0 812 049
EP-A- 0 832 800
EP-A- 0 838 788
WO-A-96/02883
WO-A1-98/11700
US-A- 3 623 014
US-A- 4 534 025
US-A- 4 694 408
US-A- 5 278 759
US-A- 5 313 584
US-A- 5 351 041
US-A- 5 377 322
US-A- 5 481 456

- **INOUE ET AL.: "Multiplex systems for automotive integrated control" MULTIPLEX TECHNOLOGY APPLICATIONS IN VEHICLE ELECTRICAL SYSTEMS, XP002062364 cited in the application**
- **AZUMA ET AL: "Development of a Class C multiplex control IC" MULTIPLEX TECHNOLOGY APPLICATIONS IN VEHICLE ELECTRICAL SYSTEMS, XP002062793 cited in the application**
- **MATHONY ET AL.: "Network architecture for CAN" MULTIPLEX TECHNOLOGY APPLICATIONS IN VEHICLE ELECTRICAL SYSTEMS, XP002062362 cited in the application**
- **SZYDLOWSKI: "a gatway for CAN-specification 2.0 non-passive devices" AMULTIPLEX TECHNOLOGY APPLICATIONS IN VEHICLE ELECTRICAL SYSTEMS, XP002062365 cited in the application**
- **NEUMANN ET AL.: "Open systems and Interfaces for distributed electronics in cars (OSEK)" MULTIPLEX TECHNOLOGY APPLICATIONS IN VEHICLE ELECTRICAL SYSTEMS, XP002062366 cited in the application**
- **EMAUS: "Aspects and issues of multiple vehicle networks" MULTIPLEX TECHNOLOGY APPLICATIONS IN VEHICLE ELECTRICAL SYSTEMS, XP002062363 cited in the application**
- **PÖTTIG W.; SCHMIDT A.: 'Universelles, sicheres und fehlertolerantes Multicontoller-System; Anwendung in einem vollautomatischen FahrzeugleitsysteM', VDI-Berichte 612: "Elektronik im Kraftfahrzeug"; VDI-Verlag GmbH, Düsseldorf (DE), 1986, pages 219-232 XP002281130**
- **REMBOLD U.; ARMBRUSTER K.; ÜLZMANN W.: 'Interface Technology for Computer-Controlled Manufacturing Processes', Marcel Dekker Inc. New York (US), 1983, pages 297-306**

Printed by Jouve, 75001 PARIS (FR)

(Cont. next page)

- **GEBHARDT K.; VON SCHWEINITZ M.: 'Das Opel-Diagnose-Konzept aus der Sicht des Entwicklers - Status und zukünftige Anforderungen' VDI-BERICHTE no. 687, 1988, DOSSELDORF (DE), pages 349 - 364, XP002333464**

Description

[0001] This invention relates to a fault resilient automobile control system, an automobile comprising such a system, a method of operating an automobile control system and a computer programmed to perform the steps of the method.

BACKGROUND OF THE INVENTION

[0002] Modem automobiles are typically equipped with multiple independent electronic components. For instance, most modem automobiles have an electronic engine control system, a computerized antilock braking system (ABS), a vehicle safety system, a lighting control system, a climate control subsystem, and a sound system. The engine control system usually employs an electronic controller to maximize fuel economy and minimize harmful emissions. The antilock braking system uses electronic sensors and microprocessors to slow an automobile at an optimal rate while preventing skidding. The vehicle safety system has a crash response controller that is triggered during a crash to deploy one or more airbags.

[0003] Some recent automobile models are equipped with a navigation system that employs a global positioning system (GPS) receiver to receive positioning signals from a satellite network. The navigation system computes coordinates that locate the vehicle over the surface of the earth with regard to longitude, latitude, and altitude. Cellular communication systems have also been introduced into automobiles to enable the driver or occupant to transact telephone calls from their vehicle. Most late model automobiles are also constructed with a diagnostic system that analyzes the performance of the automobile engine, air and heating system, and other components (1996 or later for OBD II, 1993 or later for OBD I).

[0004] While these various electronic components have proven useful, there is a drawback in that all of them are entirely separate and independent from one another. Generally, these subsystems are supplied by different manufacturers. These disparate components often employ proprietary, dedicated processors or ASICs (application specific integrated circuits) that have different system architectures and execute incompatible proprietary software. The components have limited or no communications with one another.

[0005] Some strides have been made to integrate the components. Typically, the proposals call for each of the distributed components to be connected to a data bus, such as a CAN (Controller Area Network) protocol bus. Designers have theorized different multiplexing protocols and token passing protocols to facilitate communication over the bus. For more information on these proposals, the reader is directed to the following articles which appear in a publication from the Society of Automotive Engineers (SAE): Inoue et al., "Multiplex Systems for Automotive Integrated Control," Multiplex Technology Applications in Vehicle Electrical Systems, SP-954, No. 930002, copyright 1993; Azuma et al., "Development of a Class C Multiplex Control IC," Multiplex Technology Applications in Vehicle Electrical Systems, SP-954, No. 930003, copyright 1993; Mathony et al. "Network Architecture for CAN," Multiplex Technology Applications in Vehicle Electrical Systems, SP-954, No. 930004, copyright 1993; Szydolowski, "A Gateway for CAN Specification 2.0 Non-Passive Devices," Multiplex Technology Applications in Vehicle Electrical Systems, SP-954, No. 930005, copyright 1993; Neumann et al., "Open Systems and Interfaces for Distributed Electronics in Cars (OSEK)," Automotive Multiplexing Technology, SP-1070, No. 950291, copyright 1995; and Emaus, "Aspects and Issues of Multiple Vehicle Networks," Automotive Multiplexing Technology, SP-1070, No. 950293, copyright 1995.

[0006] While there has been some progress at interconnecting electronic components in a distributed system via a communication link, there is no commonly accepted standard for the main vehicle system bus and bus interface. Additionally, even in the distributed architecture, the electronic components are individually vulnerable to unrecoverable failure. When a component experiences an electronics failure, such as a failed controller, the component is either rendered entirely useless or reduced to a safe, but otherwise sub-optimally performing unit.

[0007] The inventors have developed a fault-resilient system which solves these problems.

[0008] Pöttig, W., Schmidt, A.: "Universelles, sicheres und fehlertolerantes Multicontroller-System; Anwendung in einem vollautomatischen Fahrzeugleitsystem"; VDI-Berichte No.612, VDI-Verlag Düsseldorf, 1996, pages 219-232, describe a universal reliable and failure-tolerant multi-controller system in an automatic vehicle guiding system. For safety reasons, redundancies are built into these systems. It describes eight different types of redundancy including centralised redundancy in which, in the case of a failure, all system functions are taken over by a functional unit which would be sufficient in its own right to maintain the overall function. In example 1, of Figure 3, it is clear that the system includes two control units with the second control unit providing a backup to the first. The systems are primarily concerned with the local processor units operating in a fail safe state rather than being controlled from elsewhere.

SUMMARY OF THE INVENTION

[0009] This invention concerns a fault-resistent automobile control system that integrates diverse and separate automobile components and tolerates component failure.

[0010] In a first aspect of the invention, a fault-resilient automobile control system for an automobile having multiple electronic automobile components, each electronic automobile component having a local controller for con-

trolling operation of the electronic automobile component, each local controller storing driver software, the controller being arranged so that, when executing the software, the local controller controls the electronic automobile component, the automobile control system comprising: a master control unit electrically coupled to the electronic automobile components, the master control unit having a computer processor, the electronic components each being arranged to register with the master control unit and to programme the master control unit during initialisation or upon addition to the system, by downloading the driver software for the local controllers and by storing the driver software in the master control unit, the computer processor thereby being programmed to perform control tasks of the local controllers so that in an event that one of the local controllers fails, the computer processor executes the driver software of the failed local controller so that the master control unit controls the electronic automobile component in place of the failed local controller, the master control unit being arranged during operation of the control system to monitor continuously for failure of a local controller, wherein each electronic automobile component comprises switching logic, the switching logic being arranged to selectively route data to the local controller, or to the master control unit if the local controller fails.

[0011] In a second aspect of the invention, an automobile comprises a fault-resilient automobile control system according to the first aspect of the invention.

[0012] In a third aspect of the invention, a method of operating an automobile control system for an automobile having multiple electronic automobile components, each electronic automobile component having a local controller for controlling operation of the associated electronic automobile components and switching logic for selectively routing data to the local controller or to the master control unit if the local controller fails, each local controller storing driver software, the driver software arranged so that when executed by the local controller the local controller controls the electronic automobile component, the automobile control system comprising a master control unit coupled to the electronic automobile components, the master control unit having a computer processor, the method comprising the following steps: (1) during initialisation or as the electronic automobile components are added to the system, registering the electronic components with the master control unit and downloading to the master control unit the driver software of the local controllers; (2) storing the driver software of the local controllers on the master control unit (3) continuously monitoring the local electronic controller for their failure; and (4) in an event that one of the electronic controllers fails, executing the driver software of the failed local controller and thereby remotely controlling the associated component from the computer processor.

[0013] In a fourth aspect of the invention there is computer programmed to perform the steps of the method of the third aspect of the invention.

[0014] A number of preferred and advantageous features of the invention are referred to in the dependent claims.

[0015] According to an embodiment disclosed herein, the fault-resilient automobile control system includes a master control unit (MCU) electrically coupled via a data communications bus to the electronic automobile components. The master control unit has a computer processor programmed to manage data flow over the data communications bus among the electronic automobile components. The MCU defines and synchronizes initialization of the bus communications.

[0016] According to another embodiment disclosed herein, the MCU maintains a routing table to facilitate resource and information sharing among the components. The routing table is constructed during initialization to define how data derived at one electronic component is routed to one or more other components. During operation, the MCU collects data from the source electronic components and routes the data to destination electronic components according to the routing table. As an example of this data sharing, data collected by an antilock braking system when an automobile is slowing down might be routed to an automatic transmission system for use in determining whether to downshift.

[0017] According to another embodiment disclosed herein, the MCU's computer processor is programmed to perform the same functions as those performed by local controllers at the electronic components. During initialization, the driver software for all of the local controllers is downloaded and stored at the MCU. In the event that a local controller fails, the master control unit executes the driver software for the failed controller to remotely control the electronic automobile component in place of the failed local controller.

[0018] Switching logic is provided at each of the electronic components. The switching logic selectively routes data either to the local controller, assuming the controller is functioning properly, or over the data communications bus to the MCU, circumventing the controller, when the controller is not functioning properly.

[0019] According to yet another embodiment disclosed herein, the fault-resilient automobile control system has a secondary control unit (SCU) electrically coupled to the master control unit via the data communications network. The secondary control unit has a computer processor that supports many user-based components, such as an entertainment system or a cellular communications system. The SCU's computer processor is also programmed with a backup copy of the MCU's data communications code to manage the data flow among the electronic automobile components. During normal operation, the SCU is subordinate to and controlled by the MCU on the data communications bus. In the event that the master control unit fails, however, the secondary control unit assumes control of the data communications bus and manages the data flow among the electronic automobile components.

[0020] Accordingly, the fault-resilient automobile control system affords fault tolerance for all of the components as well as for the MCU itself.

[0021] According to another embodiment disclosed herein, the master control unit and the secondary control unit are general purpose computers which run an open platform multitasking operating system. The open architecture affords tremendous flexibility and adaptability to the addition of new automobile components or the reconfiguration of old components.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] The same reference numerals are used throughout the drawings to reference like components and features.

Fig. 1 is a diagrammatic illustration of a fault-resilient, automobile control system implemented in an automobile according to one exemplary aspect of this invention.

Fig. 2 is a block diagram of a master control unit employed in the automobile control system.

Fig. 3 is a block diagram of an exemplary electronic component employed in the automobile control system.

Fig. 4 is a block diagram of the secondary control unit employed in the automobile control system.

Fig. 5 is a state diagram showing initialization and execution of the automobile control system.

Fig. 6 is a block diagram of the automobile control system showing a master/slave relationship between the master control unit, the secondary control unit, and the multiple electronic components during normal operation.

Fig. 7 is a block diagram similar to Fig. 6, but showing a failure of an electronic component.

Fig. 8 is a block diagram similar to Fig. 6, but showing a failure of the master control unit.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0023] Fig. 1 shows an automobile control system 20 constructed in an automobile 22 according to one exemplary implementation of this invention. The automobile control system 20 has a master control unit (MCU) 24 and a secondary control unit (SCU) 26. A dual bus structure consisting of a primary data communications bus 28 and a secondary support bus 30 provide an infrastructure for data communications in the control system 20. The primary bus 28 may be implemented using any vehicle bus design currently employed or contemplated by automobile manufactures, such as CAN, ABUS, VAN, J1850, K-BUS, P-BUS, I-BUS, USB, P1394, and so forth. The support bus 30 may be implemented as any standard computer data bus, such as PCI, USB, P1394, and the like.

[0024] The master control unit 24 and the secondary control unit 26 are interconnected through the primary vehicle bus 28. In addition, various electronic automobile components are connected to the master control unit 24 via the primary bus 28. In this illustration, the electronic components include an antilock braking system (ABS) 32, an electronic steering system 34, and an engine control system 36. However, other components may likewise be connected to the primary vehicle bus 28, such as a security/alarm system, a diagnostic system, a lighting control system, a fuel injection system, an automatic transmission system, and so forth. In addition, the electronic components shown in Fig. 1 are intelligent components in that they each have their own local controller, typically embodied as a microprocessor. The automobile might further include non-intelligent electronic components which do not have local processing capabilities, as is explained below with reference to Figs. 6-8.

[0025] Fig. 1 shows a number of devices connected to the support bus 30. These devices include a climate control system 38, an audio system 40, a navigation system 42 with global positioning system (GPS) antenna 44, and a cellular communications system 46. Door locks and window controls 48 are also connected to the support bus 30. The secondary control unit 26 is master of the support bus 30. The SCU 26 is also configured as a server to multiple clients 50. The clients 50 can be, for example, small hand held or laptop game computers having visual display screens and audio sound cards to provide multimedia entertainment. The SCU 26 serves in-car entertainment in the form of movies and games to the clients 50 for the passengers enjoyment.

[0026] In general, during normal operation of the automobile control system 20, the master control unit 24 is the master of the primary vehicle bus 28. All electronic components 32-36, as well as the secondary control unit 26, are slaves to master control unit 24. The master control unit 24 manages data flow among the electronic components 32-36 and facilitates resource and information sharing. In addition, the master control unit 24 provides backup for the intelligent electronic components in the event that any of them fail, and also performs data processing and control functions for non-intelligent electronic components.

[0027] Fig. 2 shows the master control unit 24 in more detail. It has a computer processor 60, volatile memory 62 (e.g., RAM), and non-volatile memory 64 (e.g., ROM, Flash). The master control unit 24 also has a bus interface 66 to provide access to the primary bus 28. The master control unit 24 runs an open platform operating system 68, which is shown stored in non-volatile memory 64.

During runtime, the operating system 68 loads into volatile memory 62 and executes on processor 60. The open platform operating system 68 is preferably a real-time, multitasking operating system capable of supporting "plug-and-play" system configuration and providing high stability, security, and efficiency. One preferred operating system is a Windows® brand operating system sold by Microsoft Corporation, such as Windows CE® or Windows NT® operating systems.

[0028] The operating system 68 has network management capabilities which enable the master control unit 24 to manage data flow over the primary bus 28 among the electronic components 32-36 and the secondary control unit 26. The master control unit 24 initializes the network communication and register subsystem, and handles component configuration. During operation, the master control unit 24 preferably controls the data flow in a deterministic manner, accepting only predefined data from the electronic components. This is advantageous in that the master control unit provides protection to individual electronic components that are connected on the primary vehicle bus 28 against unexpected or unauthorized commands. In addition, the networking capabilities enable the master control unit 24 to monitor for deletion or addition of electronic components to the primary bus 28.

[0029] The MCU 24 contains driver software, referenced generally as number 70, for all of the electronic components connected to the primary bus 28. The electronic components register with the MCU 24 during initialization, or as they are added to the bus. The components' software code 70 may already exist in the MCU memory in dynamic link library (DLL) form which can be linked to the MCU system as components are registered. If the software code of one or more components do not exist in the DLL, a part of this registration involves downloading the software code used to run the components over the primary bus 28 to the master control unit 24. Fig. 2 shows driver software 70 for local controllers LC(1), LC (2), ... LC(N) of intelligent electronic components (i.e., components with local controllers) stored in the non-volatile memory 64. Fig. 2 also shows executable code for the non-intelligent components NIC(1), NIC(2), ..., NIC (M) (i.e., components without local controllers), referenced general as number 72, stored in non-volatile memory 64.

[0030] In the instance that a local controller of an intelligent component fails, the MCU 24 assumes control of that component and assigns to the failed component a highest execution priority to ensure uninterrupted performance. For instance, if the processor in the ABS fails, the MCU 24 runs the local controller driver, say driver LC (1), to perform the functions of the failed processor for the antilock braking system. Switching logic is provided at the failed component to transfer control to the MCU. Once the MCU 24 assumes control of a component, the MCU 24 performs its data flow management functions on a resource available basis.

[0031] The operating system 68 is a real-time, deterministic operating system that has the processing power capable of concurrently supporting multiple critical components. In the event that multiple components fail, the MCU 24 employs a priority table 74 which specifies an ordered ranking for executing the failed devices. The priority table 74 is constructed during initialization as the components register with the MCU 24. During registration, the MCU 24 assigns a priority rating to each of the electronic automobile components and stores the association in a table in the non-volatile memory 64.. The priority rating is associated through the table's data structure to identifiers for the driver software 70 and executable code 72. The priority is predetermined by the automobile manufacturer based upon which components register with the MCU 24. It is noted that the priority table 74 may alternatively be reconstructed from scratch each start cycle and maintained in volatile memory 62.

[0032] Once constructed, the priority table 74 establishes a priority of operation in the event that more than one component fails. The priority table 74 assigns processing resources disproportionately to the highest priority rated component first, followed in order by the lower priority rated components. For instance, the driver software for the antilock braking system might be assigned the highest priority rating to ensure that the MCU 24 has sufficient resources to handle the braking system in the event it fails, even though other components (such as the security system) might also fail during that time. In one implementation, the components are assigned a "critical" rating, meaning that they are given the highest priority available, a "normal" rating, meaning that they can be given a lower priority if a critical component concurrently fails, or a "lowest" rating, meaning that they will receive MCU resources only after all components with higher priority have been handled.

[0033] The MCU 24 also maintains a routing table 76 in volatile memory 62. The routing table 76 is constructed during initialization to define which data is passed and shared among the active electronic components. For instance, the table might define a data structure having a source field that contains an identifier of an electronic component from where certain data is generated, and a destination field that contains a list of one or more components to which the certain data is to be routed by the MCU 24. For instance, data collected by the ABS 32 (i.e., a source component) concerning wheel speed might be routed to the automatic transmission control system and the fuel injection control system (i.e., destination components). The source and destination fields are correlated in the table 76. During operation, the MCU 24 collects data from the electronic components identified in the source fields (such as the ABS), indexes the routing table 76 to corresponding destination fields, and routes the data to the electronic components (such as the automatic transmission control system or fuel injection system) listed in the corresponding destination fields. The routing table enables the MCU 24 to facilitate data sharing among the components.

[0034] Fig. 3 shows an exemplary construction of an intelligent electronic automobile component, referenced generally as number 80. The automobile component 80 generally comprises a mechanical device 82 (such as brakes, engine, transmission, etc.) which is controlled through an electronically-controlled actuator 84. A local controller 86 is coupled through a driver 88 to send electronic command signals that control the actuator and hence, the mechanical apparatus 82. The local controller 86 can be implemented as a microprocessor, digital signal processor, dedicated ASIC (application specific integrated circuit), or the like. A sensor 90 monitors the mechanical apparatus 82 and generates data indicative of operation to provide feedback information to the local controller 86. The local controller 86 also has an interface to the primary vehicle bus 28. This construction of the electronic automobile component is customary and known in the art.

[0035] An aspect of this invention is to modify the existing electronic automobile component 80 to include switching logic 92. In the Fig. 3 illustration, the switching logic 92 is interfaced between the local controller 86 and the driver 88 and sensor 90. The switching logic 92 also has its own connection to the primary bus 28 which bypasses the local controller 86. The switching logic 92 selectively routes data received from the sensor 90 to either the local controller 86 or directly to the primary bus 28. The switching logic 92 directs the data to the local controller 86 when the controller is functioning properly. In the event that the controller is not functioning properly, however, the switching logic 92 routes data flow to the bus 28, circumventing the failed local controller 86, so that the MCU 24 can control the component over the primary bus 28.

[0036] Fig. 4 shows the secondary control unit 26 in more detail. The secondary control unit 26 is preferably a general purpose computer capable of supporting multiple applications. The SCU 26 has a processor 100 (e.g., SH3 from Hitachi, Ltd. or Pentium® microprocessor from Intel Corporation), volatile memory 102 (e.g., RAM), and non-volatile memory 104 (e.g., ROM, Flash, hard disk, etc.). The SCU 26 has a primary bus interface 106 to provide access to the primary vehicle bus 28 and a support bus interface 108 to provide access to the support bus 30.

[0037] The SCU 26 runs an open platform operating system 110 which supports multiple applications. Using an open platform operating system and an open computer system architecture, various software applications and hardware peripherals can be supported by the SCU 26 on the support bus 30. This is advantageous in that the software applications do not need to be dedicated to specially designed embedded systems. The open hardware architecture is preferably running a multitasking operating system that employs a graphical user interface. One preferred operating system is a Windows® brand operating system sold by Microsoft Corporation, such as Windows 95® or Windows NT® or other derivative versions of Windows®. A multitasking operating system allows simultaneous execution of multiple applications.

[0038] The SCU 26 might also include at least one storage drive-such as a CD ROM drive, PC Card drive, or a floppy disk drive-which permits use of portable storage media. A CD ROM drive enables application-related CDs, as well as musical, video, game, or other types of entertainment CDs. The SCU 26 is constructed and sized to mount in the dashboard of the automobile. A detailed explanation of one suitable construction of a secondary control unit 26 is described in U.S. Patent Application Serial Number 08/564,586, entitled "Vehicle Computer System," which was filed November 29, 1995, in the names of Richard D. Beckert, Mark M. Moeller, and William Wong. This application is assigned to Microsoft Corporation and is hereby incorporated by reference.

[0039] The secondary control unit 26 is slave to the master control unit 24 on the vehicle bus 28, but is a master to clients 50 and other electronic components 38-48 connected to the support bus 30. dashboard or other suitable location. The SCU 26 can function as a server to the clients 50, such as to serve games, music, movies or other forms of entertainment.

[0040] The SCU 26 maintains an up-to-date copy of executable code 112 run by the MCU 24 to manage data flow among the components. The MCU code 112 is downloaded to the SCU 26 during initialization and stored in the non-volatile memory 84. In the event that the MCU 24 fails, the secondary control unit 26 executes the MCU code 112 to assume the master responsibility of data flow management on the primary bus 28.

[0041] Fig. 5 shows a state diagram of the automobile control system. The startup is triggered by turning on power to the automobile. At state 120, the master control unit 24 runs an initialization procedure to boot the operating system and loads from non-volatile memory all of the driver software 70 for intelligent components and executable code 72 for non-intelligent components into the volatile memory. These software programs correspond to components that are pre-known to the MCU 24 through previous registration. At state 122, the MCU 24 runs a dynamic configuration procedure which checks if any new component has been added to or old components removed from the primary vehicle bus. The MCU 24 polls the existing components and sends out requests for new components. Components which are still attached and functioning respond to the MCU 24. New components also respond and subsequently register with the MCU 24. Components that have been removed, of course, do not respond to the polling signals.

[0042] Once the components are identified and accounted for, the MCU 24 constructs the priority table 74 and stores it in non-volatile memory 104. The MCU 24 also constructs the routing table 76 based upon the existing active components.

[0043] At state 124, the MCU 24 downloads a copy of its code to the SCU 26 over the primary bus 28. Following this initialization sequence, the MCU enters its normal

operating state 126. If the MCU fails, control is shifted back to the SCU 26 (as indicated by the MCU FAIL arrow). If the MCU is subsequently restored, control is returned to the MCU 24 (as indicated by the READY arrow).

[0044] Also at state 126, the MCU 24 continuously monitors for failure of any electronic components. If the MCU 24 detects a component failure, the MCU 24 reconfigures the routing and priority tables dynamically and assumes control of the failed component (as indicated by the COMPONENT FAIL arrow back to state 122).

[0045] Figs. 6-8 show the fault tolerant control strategies implemented by the automobile control system. Fig. 6 shows the automobile control system 20 as having the MCU 24 and two intelligent electronic components 80(1), 80(2) and two non-intelligent components 130(1), 130(2) connected to the primary bus 28. The system further includes the SCU 26 connected to both the primary bus 28 and the support bus 30, and two clients 50 and the audio system 40 coupled to the support bus 30.

[0046] During normal operation, the master control unit 24 is master to the primary bus 28 and to the secondary control unit 26. The master control unit 24 manages the data flow over the primary bus 28 and performs the data processing and control functions for the non-intelligent components 130(1), 130(2). The MCU 24 continuously monitors the intelligent components 80(1), 80(2) to detect whether the local controllers 86(1), 86(2) are functioning properly. The MCU 24 and SCU 26 operate cooperatively, or independently, of one another in normal circumstances, except that the SCU 26 checks with the MCU 24 at regular intervals for signs of failure.

[0047] Because the MCU 24 controls all data communications on the primary bus 28, it also maintains the security and integrity of the primary bus 28 through continuous monitoring of messages sent by the electronic components, and particularly the SCU 26 since it is an open system. Should the SCU 26 become corrupted and attempt to gain unauthorized control of any electronic component on the primary bus 28, the MCU 24 will disable communication from the SCU 26 by altering its status in the configuration and routing tables. This action relegates the SCU 26 to a passive device which only receives messages and cannot transmit them over the primary bus 28. The MCU 24 will then attempt to select another candidate to designate as a surrogate secondary control unit, going through the process states 122 and 124 as described in Fig. 5.

[0048] Fig. 7 shows a case in which a local controller 86(1) fails. In the instance the local controller 86(1) fails, the switching logic 92(1) diverts data flow from the local controller 86(1) directly to the primary bus 28. The master control unit 24 assumes control of the component 80(1) using the component driver 86(1)' stored at the MCU 24. The MCU 24 assigns the highest execution priority to ensure uninterrupted performance of the failed component. For instance, if the microprocessor in the ABS fails, the MCU 24 assumes the functions of the ABS microprocessor and provides uninterrupted service to the ABS component. The MCU 24 continues to manage data flow between components on a resource available basis.

[0049] Fig. 8 shows a case in which the MCU 24 fails. The SCU 26 detects when the MCU 24 fails through continuous monitoring or alternatively through a non-maskable interrupt generated by the MCU 24 immediately prior to failure. When the MCU fails, the SCU 26 assumes the basic data flow management and control functions of the MCU 24, as well as the processing functions for non-intelligent components 130(1) and 130(2). The SCU 26 runs the local copy of the MCU code 26' to become the surrogate master of the primary bus 28 and the components 80(1), 80(2), 130(1), 130(2) connected thereto. In this implementation, however, the SCU 26 does not assume the functions of any failed local controller of a component on the vehicle bus. To ensure uninterrupted service to the components on the primary bus 28, the SCU 26 assigns the highest priority to performance of the basic data flow management and control function of the failed MCU 24, and performs all other functions on a resource available basis.

[0050] The fault-resilient automobile control system offers many advantages. It integrates the electronic components and facilitates data sharing and communication among them. The system also provides single point fault-tolerance in that every component and the master control unit can fail one time without loss of services. The system affords tremendous flexibility when installing system components in a vehicle. Each component or bus can be installed as an upgrade feature to provide full system functionality. When a new component is installed, a driver for that component is merely loaded at the MCU to enable backup in the event of failure.

[0051] The invention has been described in language more or less specific as to structure and method features. It is to be understood, however, that the invention is not limited to the specific features described, since the means herein disclosed comprise exemplary forms of putting the invention into effect.

Claims

1. A fault-resilient automobile control system (20) for an automobile having multiple electronic automobile components (32,34,36),

each electronic automobile component (32,34,36) having a local controller (86) for controlling operation of the electronic automobile component, each local controller (86) storing driver software, the controller (86) being arranged so that, when executing the software, the local controller (86) controls the electronic automobile component (32,34,36),

the automobile control system (20) comprising: a master control unit (24) electrically coupled to the electronic automobile components, the master control unit (24) having a computer processor (60), the electronic components (32,34,36) each being ar-

ranged to register with the master control unit (24) and to programme the master control unit (24) during initialisation or upon addition to the system, by downloading the driver software for the local controllers and by storing the driver software in the master control unit (24), the computer processor thereby being programmed to perform control tasks of the local controllers (86) so that in an event that one of the local controllers (86) fails, the computer processor (60) executes the driver software of the failed local controller so that the master control unit (24) controls the electronic automobile component (32,34,36) in place of the failed local controller, the master control unit (24) being arranged during operation of the control system to monitor continuously for failure of a local controller (86),
wherein each electronic automobile component (32,34,36) comprises switching logic, the switching logic being arranged to selectively route data to the local controller (86), or to the master control unit (24) if the local controller (86) fails.

2. A fault-resilient automobile control system as recited in claim 1, wherein the master control unit (24) has an open platform operating system executing on the computer processor (60).

3. A fault-resilient automobile control system as recited in claim 1 or claim 2, wherein the master control unit (24) has a multitasking operating system executing on the computer processor (60).

4. A fault-resilient automobile control system as recited in any one of the preceding claims, wherein the master control unit (24) facilitates data communication among the electronic automobile components (32,34,36).

5. A fault-resilient automobile control system as recited in any one of the preceding claims, wherein the master control unit (24) maintains a routing table (76) which the master control unit (24) employs to route data detected by one electronic automobile component (32,34,36) to one or more other electronic automobile components (32,34,36).

6. A fault-resilient automobile control system as recited in any one of the preceding claims, wherein the master control unit (24) has a memory (64) and maintains a priority table (74) in the memory (64), the priority table (74) associating a priority rating with corresponding ones of the electronic automobile components (32,34,36), the master control unit (24) handling the tasks of one or more failed local controllers (86) in an order according to the priority ratings of the electronic automobile components (32,34,36) in the priority table (74).

7. A fault-resilient automobile control system as recited in any one of the preceding claims, in which the electronic automobile components (32,34,36) further include non-intelligent components (130) configured without local controllers, and wherein the master control unit (24) performs data processing and control functions for the non-intelligent components (130).

8. A fault-resilient automobile control system as recited in any preceding claim, further comprising a data communications network interconnecting the electronic automobile components (32,34,36) and the master control unit (24).

9. A fault-resilient automobile control system according to claim 8, wherein the master control unit (24) is electrically coupled to the electronic automobile components via the data communications network and is programmed to manage data flow over the data communications network among the electronic automobile components (32,34,36).

10. A fault-resilient automobile control system according to any one of the preceding claims, further comprising a secondary control unit (26) electrically coupled to the master control unit (24), the secondary control unit (26) having a computer processor (100) programmed to manage the data flow among the electronic automobile components (32,34,36) in the event that the master control unit (24) fails.

11. A fault-resilient automobile control system as recited in claim 10, wherein the secondary control unit (26) has an open platform, multi-tasking operating system executing on a computer processor (100) of the secondary control unit (26).

12. A fault-resilient automobile control system as recited in claim 10 or 11, further comprising:

a dual bus data structure having a primary bus (28) and support bus (300;
the primary bus (29) interconnecting the electronic automobile components (32,34,36), the master control unit (24), and the secondary control unit (26); and
the support bus (30) being connected to the secondary control unit (26) for interfacing to one or more other devices.

13. A fault-resilient automobile control system according to any one of claims 10 to 12, wherein the master control unit (24) manages data flow among the electronic automobile components (32,34,36), and the secondary control unit (26) over a primary bus; and in the event that the secondary control unit (26) attempts to gain unauthorised control of one of the

electronic automobile components (32,34,36) on the primary bus (28), the master control unit (24) is configured to disable communication originating from the secondary control unit (26) on the primary bus (28).

14. A fault-resilient automobile control system according to any of claims 8 or 9, wherein the switching logic resident at one of the electronic automobile components (32, 34, 36) is arranged to route data to one of:

(i) the local controller (86) of the electronic automobile component where the local controller is functioning properly, or
(ii) the data communications network, circumventing the local controller (86), when the local controller (86) is not functioning properly;

wherein in an event that a local controller (86) fails, the switching logic routes data to the master control unit (24) via the data communication network bypassing the failed local controller (86) and the master control unit (24) performs the tasks of the failed local controller (86).

15. An automobile comprising a fault-resilient automobile control system as recited in any one of the preceding claims.

16. A method of operating an automobile control system (20) for an automobile having multiple electronic automobile components (32,34,36), each electronic automobile component having a local controller (86) for controlling operation of the associated electronic automobile components and switching logic for selectively routing data to the local controller (86) or to the master control unit (24) if the local controller (86) fails, each local controller storing driver software, the driver software arranged so that when executed by the local controller (86) the local controller (86) controls the electronic automobile component (32,34,36), the automobile control system comprising a master control unit (24) coupled to the electronic automobile components, the master control unit (24) having a computer processor (60), the method comprising the following steps:

(1) during initialisation or as the electronic automobile components (32,34,36) are added to the system, registering the electronic components (32,34,36) with the master control unit (24) and downloading to the master control unit (24) the driver software of the local controllers;
(2) storing the driver software of the local controllers on the master control unit
(3) continuously monitoring the local electronic controllers (86) for their failure; and
(4) in an event that one of the electronic controllers (86) fails, executing the driver software of the failed local controller and thereby remotely controlling the associated component from the computer processor (60).

17. A method as claimed in claim 16, the system further comprising a secondary control unit (26) electrically coupled to the master control unit (24), wherein the method further comprises the steps of:

(1) monitoring the master control unit (24); and
(2) in the event that the master control unit fails, managing the data communication amongst the local electronic controllers (86) from the secondary control unit (26).

18. A computer programmed to perform the steps of the method as recited in claim 16 or 17.

Patentansprüche

1. Fehlertolerantes Kraftfahrzeugsteuerungssystem (20) für ein Kraftfahrzeug mit einer Vielzahl von elektronischen Kraftfahrzeugkomponenten (32, 34, 36), wobei jede elektronische Kraftfahrzeugkomponente (32, 34, 36) einen lokalen Controller (86) zum Steuern des Betriebs der elektronischen Kraftfahrzeugkomponente aufweist, wobei jeder lokaler Controller (86) Treibersoftware speichert und der Controller (86) derart ausgestaltet ist, dass er bei Ausführung der Software die elektronische Kraftfahrzeugskomponente (32, 34, 36) steuert,
wobei das Kraftfahrzeugsteuerungssystem (20) umfasst: eine elektrisch mit den elektronischen Kraftfahrzeugkomponenten verbundene Master-Steuereinheit (24), die einen Computerprozessor (60) aufweist, wobei jede der elektronischen Komponenten (32, 34, 26) zum Registrieren bei der Master-Steuereinheit (24) und zum Programmieren der Master-Steuereinheit (24) während der Initialisierung und beim Hinzufügen zu dem System durch Herunterladen der Treibersoftware für die lokalen Controller und durch Speichern der Treibersoftware in der Master-Steuereinheit (24) ausgestaltet ist, wobei der Computerprozessor dabei zum Durchführen der Steueraufgaben des lokalen Controllers (86) programmiert ist, so dass in einem Falle eines Ausfalls einer der lokalen Controller (86) der Computerprozessor (60) die Treibersoftware des ausgefallenen lokalen Controllers ausführt, so dass die Master-Steuereinheit (24) die elektronische Kraftfahrzeugkomponente (32, 34, 36) statt des ausgefallenen lokalen Controllers steuert, wobei die Master-Steuereinheit (24) während des Betriebs des Steuerungssystems zum kontinuierlichen Überwachen des Ausfalls eines lokalen Controllers (86) ausgestaltet ist, worin jede elektronische Kraftfahrzeugkomponente

(32, 34, 36) eine Schaltlogik umfasst, die zum selektiven Weiterleiten von Daten zu dem lokalen Controller (86) oder zu der Master-Steuereinheit (24) bei Ausfall des lokalen Controllers (86) ausgestaltet ist.

2. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach Anspruch 1, worin die Master-Steuereinheit (24) ein Betriebssystem für offene Plattformen aufweist, das auf dem Computerprozessor (60) ausgeführt wird.

3. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach Anspruch 1 oder 2, worin die Master-Steuereinheit (24) ein Multitasking-Betriebssystem aufweist, das auf dem Computerprozessor (60) ausgeführt wird.

4. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach einem der vorangegangenen Ansprüche, worin die Master-Steuereinheit (24) Datenkommunikation zwischen den elektronischen Kraftfahrzeugkomponenten (32, 34, 36) ermöglicht.

5. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach einem der vorangegangenen Ansprüche, worin die Master-Steuereinheit (24) eine Routing-Tabelle (76) führt, die die Master-Steuereinheit (24) zum Routen von durch eine elektronische Kraftfahrzeugkomponente (32, 34, 36) detektierten Daten zu einer oder mehreren anderen elektronischen Kraftfahrzeugkomponenten (32, 34, 36) verwendet.

6. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach einem der vorangegangenen Ansprüche, worin die Master-Steuereinheit (24) einen Speicher (64) aufweist und eine Prioritätstabelle (74) in dem Speicher (64) führt, wobei über die Prioritätstabelle (74) elektronischen Kraftfahrzeugkomponenten (32, 34, 36) eine entsprechende Prioritätsbewertung zugeordnet ist, wobei die Master-Steuereinheit (24) die Aufgaben eines oder mehrerer ausgefallener lokaler Controller (86) in einer Reihenfolge gemäß der Prioritätsbewertung der elektronischen Kraftfahrzeugkomponenten (32, 34, 36) in der Prioritätstabelle (74) handhabt.

7. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach einem der vorangegangenen Ansprüche, in dem die elektronischen Kraftfahrzeugkomponenten (32, 34, 36) ferner nicht-intelligente Komponenten (130) umfassen, die ohne lokale Controller ausgebildet sind, und worin die Master-Steuereinheit (24) die Datenverarbeitung und Steuerungsfunktionen für die nicht-intelligenten Komponenten (130) durchführt.

8. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach einem der vorangegangenen Ansprüche, das zusätzlich ein Datenkommunikationsnetzwerk aufweist, das die elektronischen Kraftfahrzeugkomponenten (32, 34, 36) und die Master-Steuereinheit (24) untereinander verbindet.

9. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach Anspruch 8, worin die Master-Steuereinheit (24) elektrisch mit den elektronischen Kraftfahrzeugkomponenten über das Datenkommunikationswerk verbunden ist und zum Verwalten des Datenflusses über das Datenkommunikationsnetzwerk zwischen den elektronischen Kraftfahrzeugkomponenten (32, 34, 36) programmiert ist.

10. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach einem der vorangegangenen Ansprüche, das zusätzlich eine untergeordnete Steuereinheit (26) umfasst, die elektrisch mit der Master-Steuereinheit (24) verbunden ist, wobei die untergeordnete Steuereinheit (26) einen Computerprozessor (100) aufweist, der zum Verwalten des Datenflusses zwischen den elektronischen Kraftfahrzeugkomponenten (32, 34, 36) in dem Falle eines Ausfalls der Master-Steuereinheit (24) programmiert ist.

11. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach Anspruch 10, worin die untergeordnete Steuereinheit (26) ein Multitasking-Betriebssystem für offene Plattformen aufweist, das auf einem Computerprozessor (100) der untergeordneten Steuereinheit (26) ausgeführt wird.

12. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach Anspruch 10 oder 11, das zusätzlich umfasst:

eine doppelte Busdatenstruktur mit einem primären Bus (28) und einem Unterstützungsbus (30),

wobei der primäre Bus (29) die elektronischen Kraftfahrzeugkomponenten (32, 34, 36), die Master-Steuereinheit (24) und die untergeordnete Steuereinheit (26) untereinander verbindet und
wobei der Unterstützungsbus (30) mit der untergeordneten Steuereinheit (26) zum Bilden einer Schnittstelle für ein oder mehrere andere Geräte verbunden ist.

13. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach einem der Ansprüche 10 bis 12, worin die Master-Steuereinheit (24) den Datenfluss zwischen den elektronischen Kraftfahrzeugkomponenten (32, 34, 36) und der untergeordneten Steuereinheit (26) über einen primären Bus verwaltet und in dem Fall, dass die untergeordnete Steuereinheit (26) versucht, unberechtigte Kontrolle über eine der elektronischen Kraftfahrzeugkomponenten (32, 34, 36) auf dem primären Bus (28) zu erlangen, die Master-Steuerein-

heit (24) zum Abschalten der von der untergeordneten Steuereinheit (26) auf den primären Bus (28) kommenden Kommunikation ausgestaltet ist.

14. Fehlertolerantes Kraftfahrzeugsteuerungssystem nach Anspruch 8 oder 9, worin die auf einem der elektronischen Kraftfahrzeugkomponenten (32, 34, 36) angesiedelte Schaltlogik ausgestaltet ist zum Weiterleiten von Daten zu:

(i) dem lokalen Controller (86) der elektronischen Kraftfahrzeugkomponente, wenn der lokale Controller korrekt arbeitet oder
(ii) dem Datenkommunikationsnetzwerk unter Umgehung des lokalen Controllers (86), wenn der lokale Controller (86) nicht korrekt arbeitet,

worin in dem Fall eines Ausfalls eines lokalen Controllers (86) die Schaltlogik die Daten zu der Master-Steuereinheit (24) über das Datenkommunikationsnetzwerk durch Überbrücken des ausgefallenen lokalen Controllers (86) weiterleitet und die Master-Steuereinheit (24) die Aufgaben des ausgefallenen lokalen Controllers (86) durchführt.

15. Kraftfahrzeug, das ein fehlertolerantes Kraftfahrzeugsteuerungssystem nach einem der vorangegangenen Ansprüche umfasst.

16. Verfahren zum Betrieb eines Kraftfahrzeugsteuerungssystem (20) für ein Kraftfahrzeug mit einer Vielzahl von elektronischen Kraftfahrzeugkomponenten (32, 34, 36), wobei jede elektronische Kraftfahrzeugkomponente einen lokalen Controller (86) zum Steuern des Betriebs der zugehörigen elektronischen Kraftfahrzeugkomponenten und Schaltlogik zum selektiven Weiterleiten von Daten zu dem lokalen Controller (86) oder zu der Master-Steuereinheit (24) bei Ausfall des lokales Controllers (86) aufweist, wobei jeder der lokalen Controller Treibersoftware speichert, die derart ausgestaltet ist, dass, wenn sie durch den lokalen Controller (86) ausgeführt wird, der lokale Controller (86) die elektronische Kraftfahrzeugkomponente (32, 34, 36) steuert, wobei das Kraftfahrzeugsteuerungssystem eine mit den elektronischen Kraftfahrzeugkomponenten verbundene Master-Steuereinheit (24) umfasst, die einen Computerprozessor (60) aufweist, wobei das Verfahren die folgenden Schritte umfasst:

(1) während der Initialisierung oder bei Hinzufügen von elektronischen Kraftfahrzeugkomponenten (32, 34, 36) zu dem System, das Registrieren der elektronischen Komponenten (32, 34, 36) bei der Master-Steuereinheit (24) und das Herunterladen der Treibersoftware der lokalen Controller auf die Master-Steuereinheit (24),
(2) Speichern der Treibersoftware des lokalen Controllers auf der Master-Steuereinheit,
(3) Kontinuierliches Überwachen der lokalen elektronischen Controller (86) hinsichtlich deren Ausfall und
(4) in dem Fall, dass einer der elektronischen Controller (86) ausfällt, das Ausführen der Treibersoftware des ausgefallenen lokalen Controllers und **dadurch** das entfernte Steuern der zugehörigen Komponente von dem Computerprozessor (60) aus.

17. Verfahren nach Anspruch 16, wobei das System zusätzlich eine mit der Master-Steuereinheit (24) elektrisch verbundene untergeordnete Steuereinheit (26) umfasst, worin das Verfahren zusätzlich die folgenden Schritte umfasst:

(1) Überwachen der Master-Steuereinheit (24) und
(2) in dem Fall, dass die Master-Steuereinheit ausfällt, das Verwalten der Datenkommunikation unter den lokalen elektronischen Controllern (86) von der untergeordneten Steuereinheit (26) aus.

18. Computer, der zum Durchführen der Schritte des Verfahrens nach Anspruch 16 oder 17 programmiert ist.

Revendications

1. Dispositif de commande automobile tolérant aux défaillances (20) pour une automobile comportant des composants automobiles électroniques multiples (32, 34, 36),
chaque composant automobile électronique (32, 34, 36) comportant une unité de commande locale (86) destinée à commander le fonctionnement d'un composant automobile électronique, chaque unité de commande locale (86) mémorisant un logiciel pilote, l'unité de commande (86) étant agencée de sorte que, lors de l'exécution du logiciel, l'unité de commande locale (86) commande le composant automobile électronique (32,34,36)
le dispositif de commande automobile (20) comprenant: une unité de commande maître (24) couplée électriquement aux composants automobiles électroniques, l'unité de commande maître (24) comportant une unité de traitement par ordinateur (60), les composants électroniques (32, 34, 36) étant chacun agencés afin de correspondre avec l'unité de commande maître (24) et de programmer l'unité de commande maître (24) au cours de l'initialisation ou lors de l'ajout au dispositif, par téléchargement du logiciel pilote pour les unités de commande locales et en mémorisant le logiciel pilote dans l'unité de comman-

de maître (24), l'unité de traitement par ordinateur étant ainsi programmée afin d'exécuter des tâches de commande des unités de commande locales (86), de sorte que, dans le cas où l'une des unités de commande locales (86) présente une défaillance, l'unité de traitement par ordinateur (60) exécute le logiciel pilote de l'unité de commande locale défaillante de sorte que l'unité de commande maître (24) commande le composant automobile électronique (32, 34, 36) à la place de l'unité de commande locale défaillante, l'unité de commande maître (24) étant agencée, au cours du fonctionnement du dispositif de commande, afin de surveiller en continu la défaillance d'une unité de commande locale (86), dans lequel chaque composant automobile électronique (32, 34, 36) comprend un circuit logique de commutation, le circuit logique de commutation étant agencé afin d'acheminer de manière sélective des données vers l'unité de commande locale (86) ou vers l'unité de commande maître (24) si l'unité de commande locale (86) présente une défaillance.

2. Dispositif de commande automobile tolérant aux défaillances selon la revendication 1, dans lequel l'unité de commande maître (24) comporte un système d'exploitation ouvert de la plate-forme s'exécutant sur l'unité de traitement par ordinateur (60).

3. Dispositif de commande automobile tolérant aux défaillances selon la revendication 1 ou 2, dans lequel l'unité de commande maître (24) comporte un système d'exploitation multitâche s'exécutant sur l'unité de traitement par ordinateur (60).

4. Dispositif de commande automobile tolérant aux défaillances selon l'une quelconque des revendications précédentes, dans lequel l'unité de commande maître (24) facilite la communication de données entre les composants automobiles électroniques (32, 34, 36).

5. Dispositif de commande automobile tolérant aux défaillances selon l'une quelconque des revendications précédentes, dans lequel l'unité de commande maître (24) entretient une table d'acheminement (76) que l'unité de commande maître (24) utilise afin d'acheminer les données détectées par un composant automobile électronique (32, 34, 36) vers un ou plusieurs autres composants automobiles électroniques (32, 34, 36).

6. Dispositif de commande automobile tolérant aux défaillances selon l'une quelconque des revendications précédentes, dans lequel l'unité de commande maître (24) comprend une mémoire (64) et entretient une table de priorité (74) dans la mémoire (64), la table de priorité (74) associant un niveau de priorité à certains correspondants des composants automobiles électroniques (32, 34, 36), l'unité de commande maître (24) prenant en charge les tâches d'une ou plusieurs des unités de commande locales défaillantes (86) dans un ordre en fonction des niveaux de priorité des composants automobiles électroniques (32, 34, 36) dans la table de priorité (74).

7. Dispositif de commande automobile tolérant aux défaillances selon l'une quelconque des revendications précédentes, dans lequel les composants automobiles électroniques (32, 34, 36) comportent, en outre, des composants non intelligents (130) configurés sans unité de commande locale, et dans lequel l'unité de commande maître (24) exécute des fonctions de traitement de données et de commande pour les composants non intelligents (130).

8. Dispositif de commande automobile tolérant aux défaillances selon une revendication précédente quelconque, comprenant, en outre, un réseau de communication de données interconnectant les composants automobiles électroniques (32, 34, 36) et l'unité de commande maître (24).

9. Dispositif de commande automobile tolérant aux défaillances selon la revendication 8, dans lequel l'unité de commande maître (24) est couplée électriquement aux composants automobiles électroniques par l'intermédiaire du réseau de communication de données et est programmée afin de gérer un flux de données sur le réseau de communication de données entre les composants automobiles électroniques (32, 34, 36).

10. Dispositif de commande automobile tolérant aux défaillances selon l'une quelconque des revendications précédentes, comprenant, en outre, une unité de commande secondaire (26) couplée électriquement à l'unité de commande maître (24), l'unité de commande secondaire (26) comportant une unité de traitement d'ordinateur (100) programmée afin de gérer le flux de données entre les composants automobiles électroniques (32, 34, 36) dans le cas où l'unité de commande maître (24) présente une défaillance.

11. Dispositif de commande automobile tolérant aux défaillances selon la revendication 10, dans lequel l'unité de commande secondaire (26) comporte un système d'exploitation multitâche ouvert de la plate-forme s'exécutant sur une unité de traitement par ordinateur (100) de l'unité de commande secondaire (26).

12. Dispositif de commande automobile tolérant aux défaillances selon la revendication 10 ou 11, comprenant, en outre:

une structure numérique à double bus comportant un bus principal (28) et un bus support (300);
le bus primaire (29) interconnectant les composants automobiles électroniques (32, 34, 36), l'unité de commande maître (24) et l'unité de commande secondaire (26); et
le bus support (30) étant couplé à l'unité de commande secondaire (26) afin d'assurer l'interface avec un ou plusieurs autres dispositifs.

13. Dispositif de commande automobile tolérant aux défaillances selon l'une quelconque des revendications 10 à 12, dans lequel l'unité de commande maître (24) gère le flux de données entre les composants automobiles électroniques (32, 34, 36) et l'unité de commande secondaire (26) sur un bus primaire ; et dans le cas où l'unité de commande secondaire (26) essaye d'obtenir une commande non autorisée de l'un des composants automobiles électroniques (32, 34, 36) sur le bus primaire (28), l'unité de commande maître (24) est configurée afin de désactiver la communication provenant de l'unité de commande secondaire (26) sur le bus primaire (28).

14. Dispositif de commande automobile tolérant aux défaillances selon l'une quelconque des revendications 8 ou 9, dans lequel le circuit logique de commutation résidant sur l'un des composants automobiles électroniques (32, 34, 36) est agencé afin d'acheminer des données vers l'un de:

(i) l'unité de commande locale (86) du composant automobile électronique dans lequel l'unité de commande locale fonctionne correctement, ou
(ii) le réseau de communication de données, contournant l'unité de commande locale (86), lorsque l'unité de commande locale (86) ne fonctionne pas correctement ;

dans lequel, dans le cas où l'unité de commande locale (86) présente une défaillance, le circuit logique de commutation achemine les données vers l'unité de commande maître (24) par l'intermédiaire du réseau de communication de données contournant l'unité de commande locale défaillante (86), et l'unité de commande maître (24) exécute les tâches de l'unité de commande locale défaillante (86).

15. Automobile comprenant un dispositif de commande automobile tolérant aux défaillances selon l'une quelconque des revendications précédentes.

16. Procédé de commande d'un dispositif de commande automobile (20) pour une automobile comportant des composants automobiles électroniques multiples (32, 34, 36), chaque composant automobile électronique comportant une unité de commande locale (86) destinée à commander le fonctionnement des composants automobiles électroniques associés et un circuit logique de commutation afin d'acheminer de manière sélective des données à l'unité de commande locale (86) ou à l'unité de commande maître (24) si l'unité de commande locale (86) présente une défaillance, chaque unité de commande locale mémorisant un logiciel pilote, le logiciel pilote étant agencé de sorte que, lorsqu'il est exécuté par l'unité de commande locale (86), l'unité de commande locale (86) commande le composant automobile électronique (32, 34, 36), le dispositif de commande automobile comprenant une unité de commande maître (24) couplée aux composants automobiles électroniques, l'unité de commande maître (24) comportant une unité de traitement par ordinateur (60), le procédé comprenant les étapes suivantes:

(1) au cours de l'initialisation ou lorsque les composants automobiles électroniques (32, 34, 36) sont ajoutés au dispositif, de mise en correspondance des composants automobiles électroniques (32, 34, 36) avec l'unité de commande maître (24) et de téléchargement vers l'unité de commande maître (24) du logiciel pilote des unités de commande locales ;
(2) de mémorisation du logiciel pilote des unités de commande locales sur l'unité de commande maître ;
(3) de surveillance continue de l'apparition d'une défaillance sur les unités de commande électroniques locales (86) ; et
(4) dans le cas où l'une des unités de commande électroniques (86) présente une défaillance, d'exécution du logiciel pilote de l'unité de commande locale défaillante et ainsi, de commande à distance du composant associé par l'unité de traitement d'ordinateur (60).

17. Procédé selon la revendication 16, le dispositif comprenant, en outre, une unité de commande secondaire (26) couplée électriquement à l'unité de commande maître (24), dans lequel le procédé comprend, en outre, les étapes de :

(1) surveillance de l'unité de commande maître (24) ; et
(2) dans le cas où l'unité de commande maître présente une défaillance, gestion des communications de données entre les unités de commande locales (86) à partir de l'unité de commande secondaire (26).

18. Ordinateur programmé afin d'exécuter les étapes du procédé selon la revendication 16 ou 17.

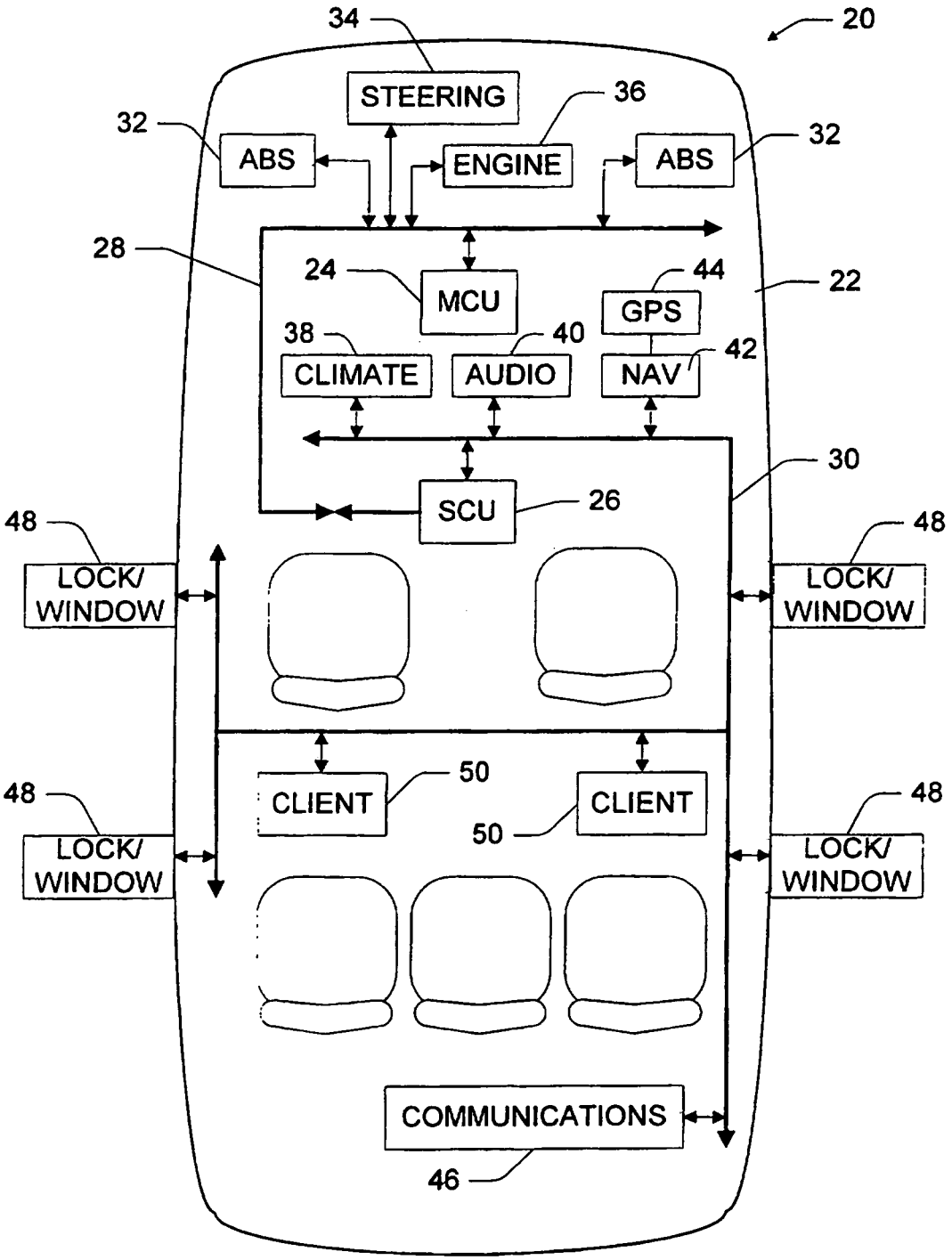
34
20
STEERING
36
32
ABS
ENGINE
ABS
32
28
24
MCU
44
GPS
22
38
40
42
CLIMATE
AUDIO
NAV
30
SCU
26
48
LOCK/
WINDOW
48
LOCK/
WINDOW
48
LOCK/
WINDOW
50
CLIENT
CLIENT
50
48
LOCK/
WINDOW
COMMUNICATIONS
46

Fig. 1

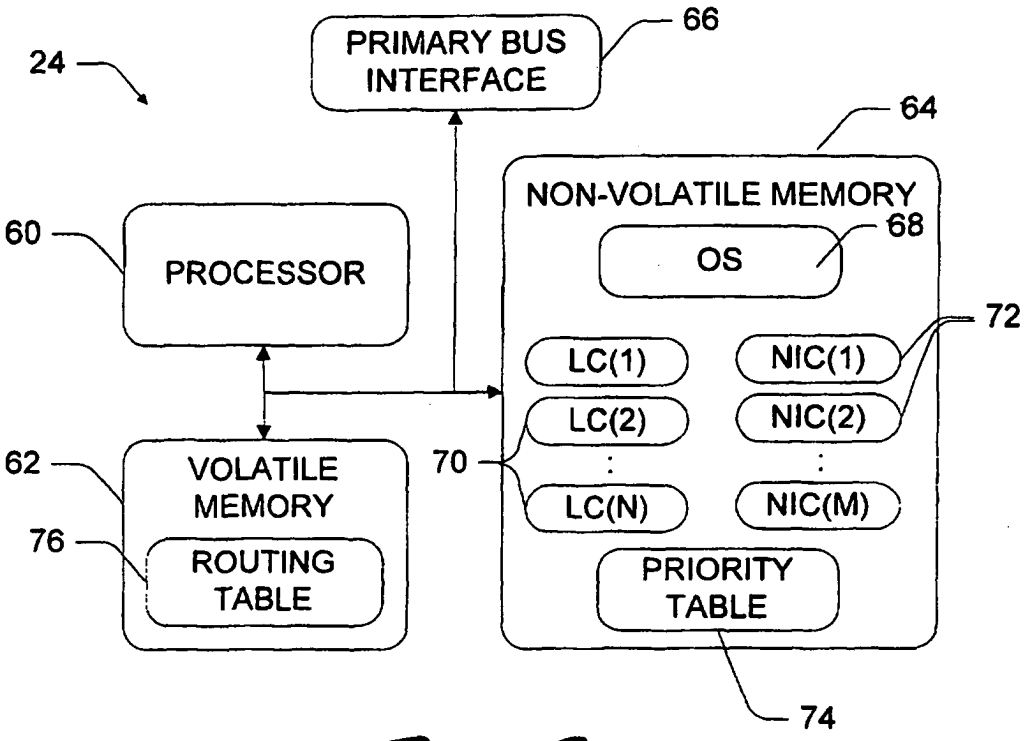
24
PRIMARY BUS INTERFACE
66
64
NON-VOLATILE MEMORY
68
OS
60
PROCESSOR
72
LC(1)
NIC(1)
LC(2)
NIC(2)
62
VOLATILE MEMORY
70
LC(N)
NIC(M)
76
ROUTING TABLE
PRIORITY TABLE
74

Fig. 2

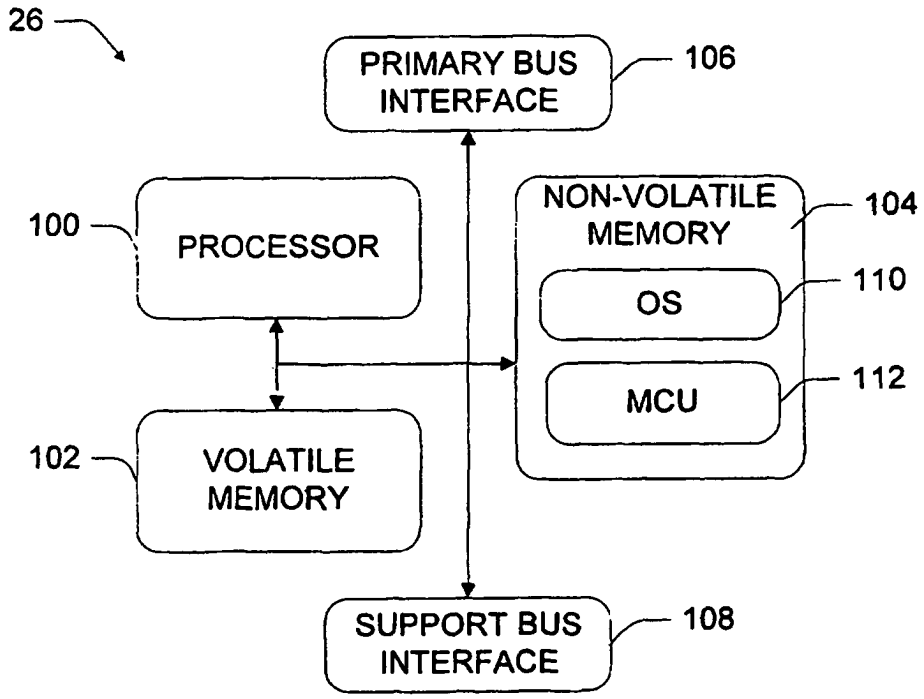
26
PRIMARY BUS INTERFACE
106
NON-VOLATILE MEMORY
104
100
PROCESSOR
OS
110
MCU
112
102
VOLATILE MEMORY
SUPPORT BUS INTERFACE
108

Fig. 4

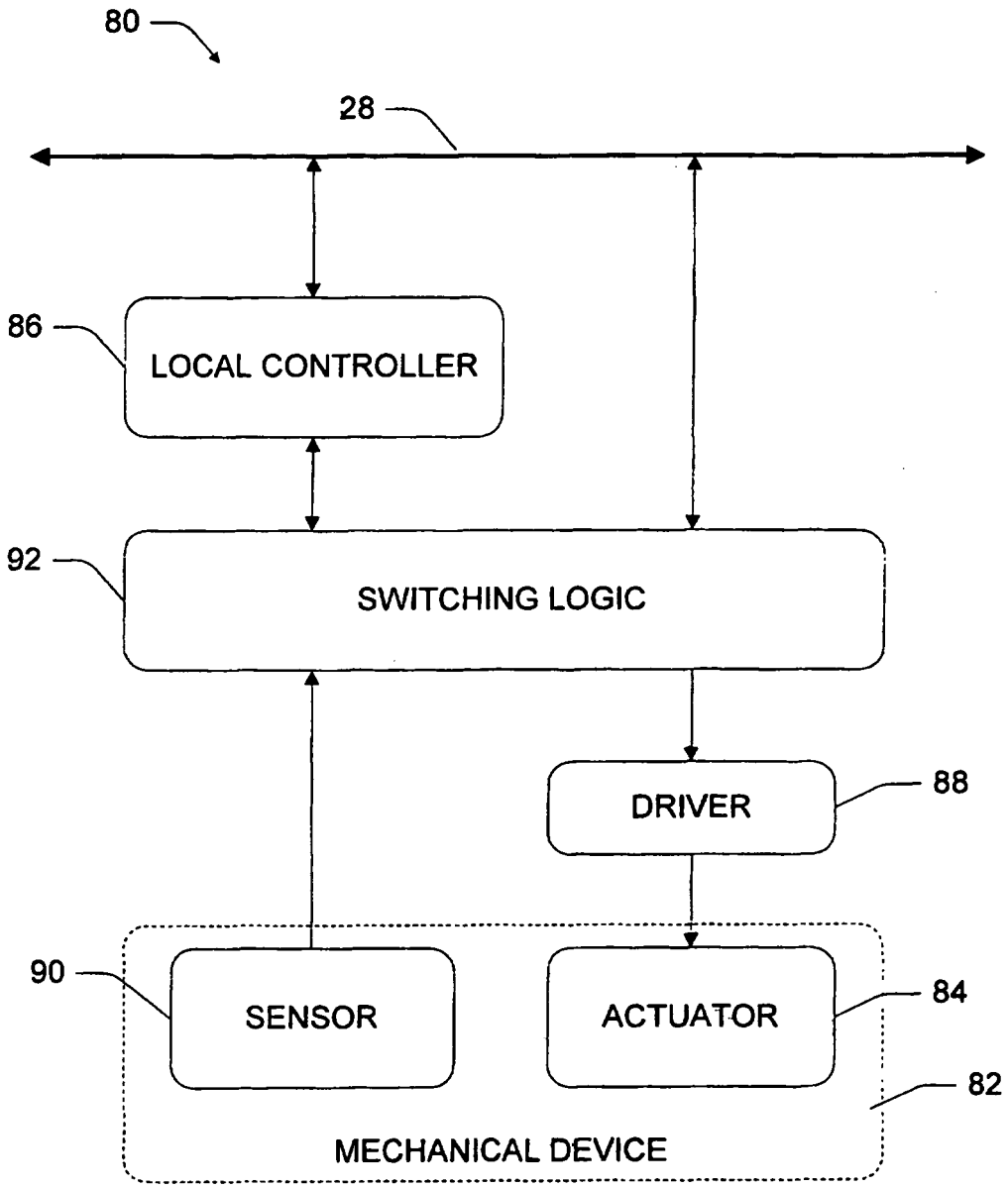
80
28
86
LOCAL CONTROLLER
92
SWITCHING LOGIC
DRIVER
88
90
SENSOR
ACTUATOR
84
82
MECHANICAL DEVICE

Fig. 3

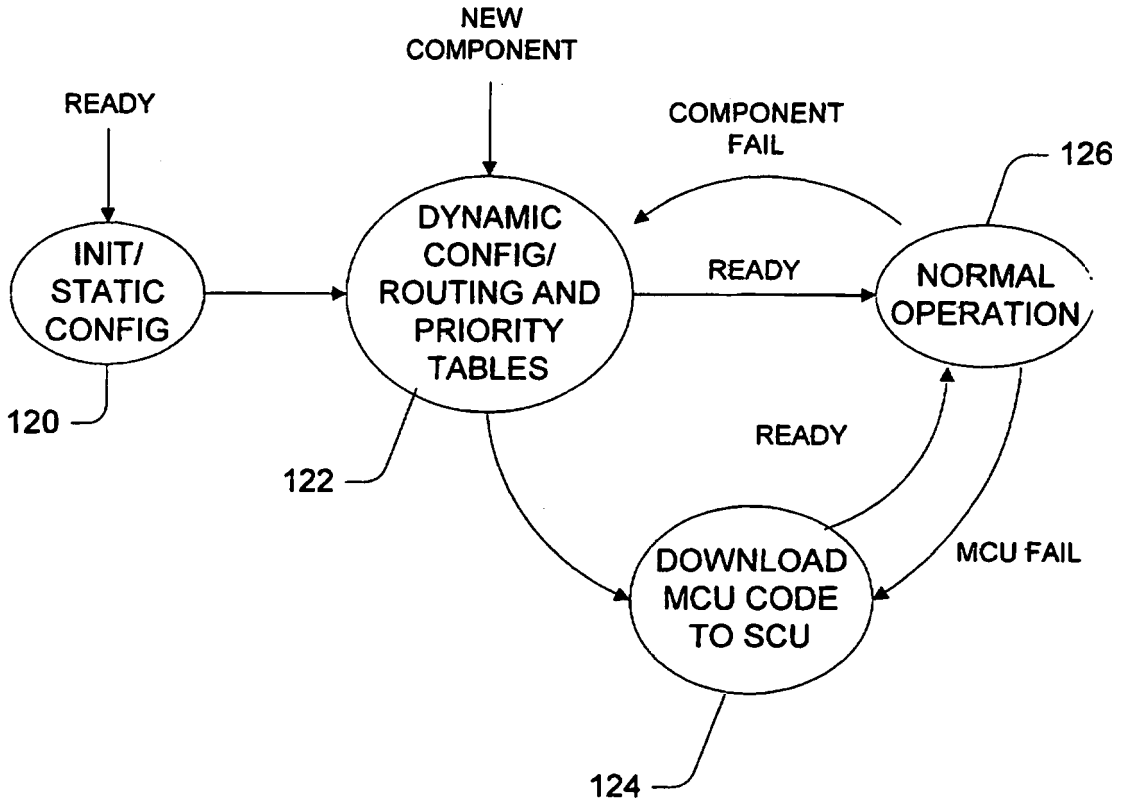
NEW
COMPONENT
READY
COMPONENT
FAIL
126
INIT/
STATIC
CONFIG
DYNAMIC
CONFIG/
ROUTING AND
PRIORITY
TABLES
READY
NORMAL
OPERATION
120
122
READY
DOWNLOAD
MCU CODE
TO SCU
MCU FAIL
124

Fig. 5

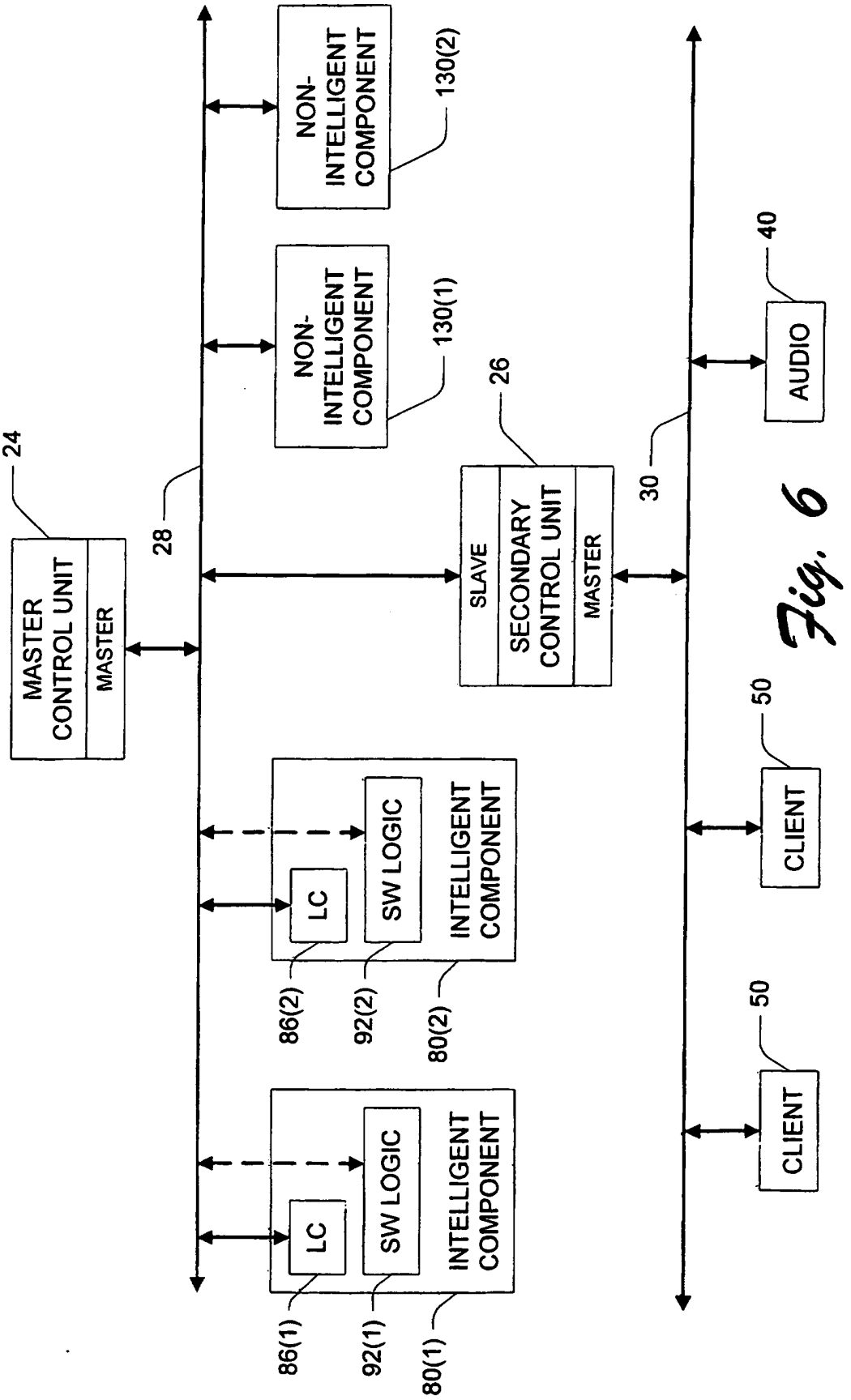
MASTER CONTROL UNIT
MASTER
24
28
NON-INTELLIGENT COMPONENT
130(2)
NON-INTELLIGENT COMPONENT
130(1)
SLAVE
SECONDARY CONTROL UNIT
MASTER
26
30
AUDIO
40
CLIENT
50
CLIENT
50
INTELLIGENT COMPONENT
LC
SW LOGIC
86(2)
92(2)
80(2)
INTELLIGENT COMPONENT
LC
SW LOGIC
86(1)
92(1)
80(1)

Fig. 6

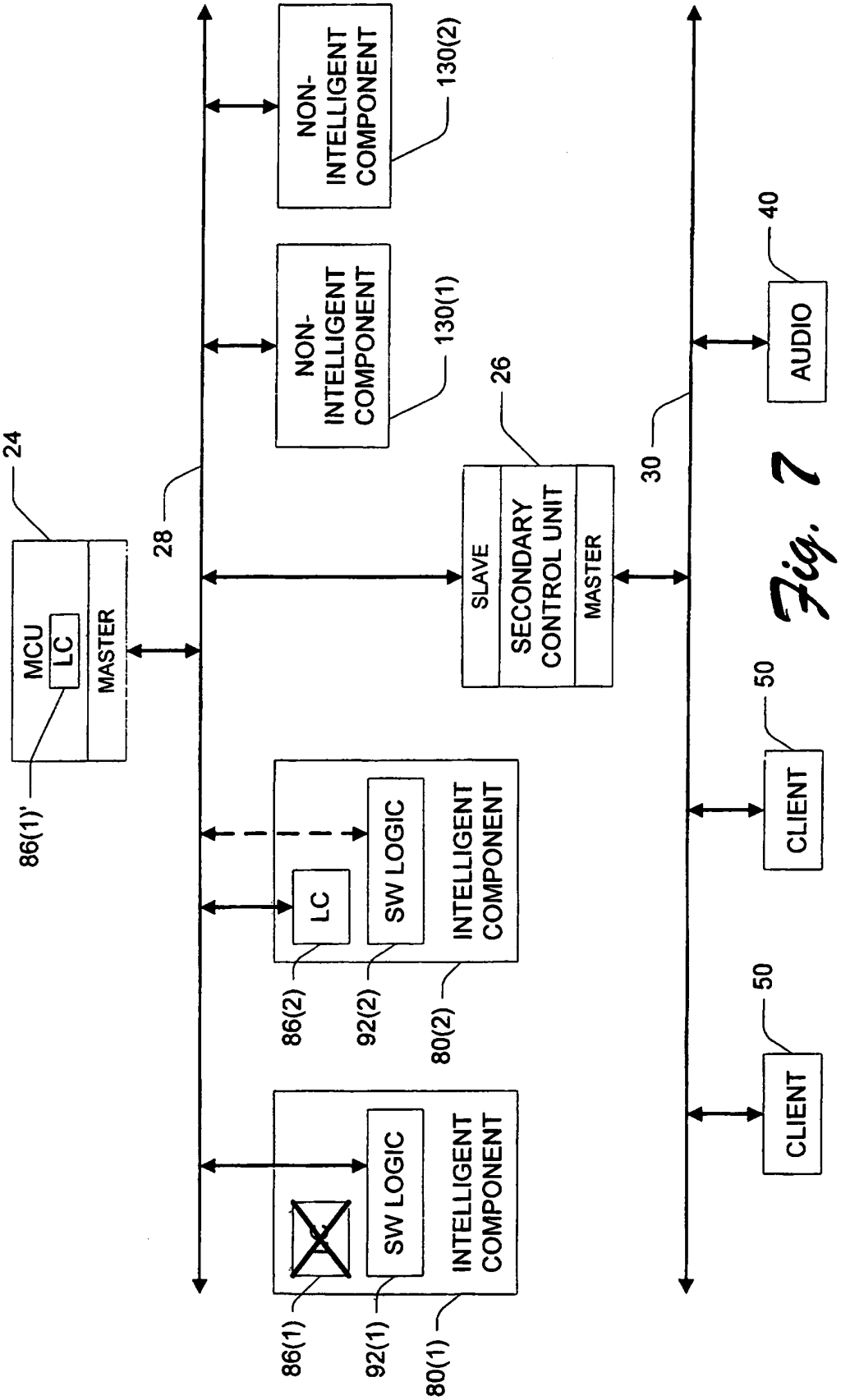
24
MCU
LC
MASTER
86(1)'
28
NON-INTELLIGENT COMPONENT
130(2)
NON-INTELLIGENT COMPONENT
130(1)
26
SLAVE
SECONDARY CONTROL UNIT
MASTER
30
40
AUDIO
INTELLIGENT COMPONENT
LC
SW LOGIC
86(2)
92(2)
80(2)
INTELLIGENT COMPONENT
SW LOGIC
86(1)
92(1)
80(1)
50
CLIENT
50
CLIENT

Fig. 7

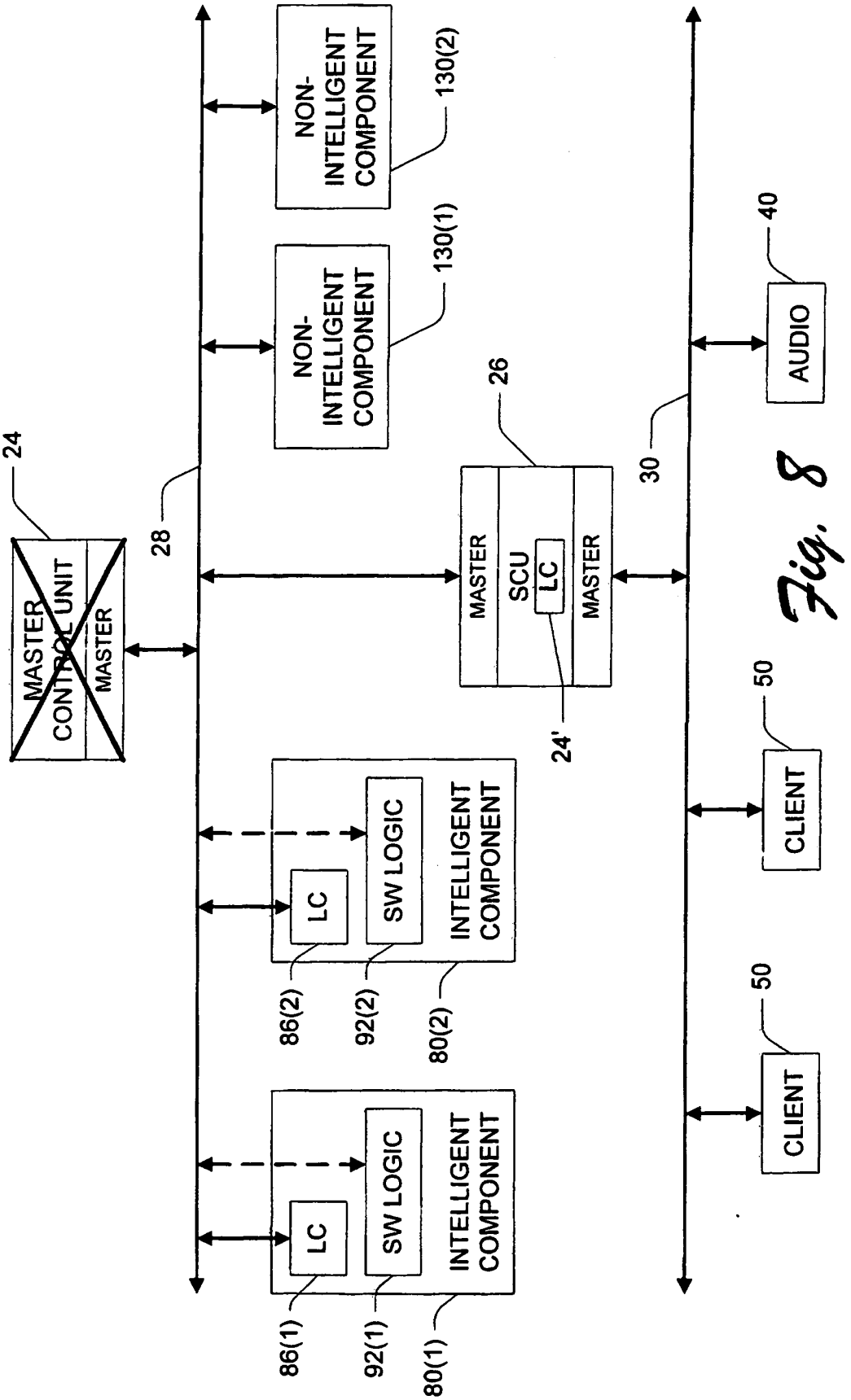
24
MASTER CONTROL UNIT
MASTER
28
NON-INTELLIGENT COMPONENT
130(2)
NON-INTELLIGENT COMPONENT
130(1)
26
MASTER
SCU
LC
MASTER
24'
30
40
AUDIO
50
CLIENT
50
CLIENT
LC
SW LOGIC
INTELLIGENT COMPONENT
86(2)
92(2)
80(2)
LC
SW LOGIC
INTELLIGENT COMPONENT
86(1)
92(1)
80(1)

Fig. 8